Travaux Pratiques

Module réseau R4

Année 2012 -2013

IUT RT, Nice Sophia-Antipolis

Énoncés

Préambule

Le module de TP de R4 aborde l'installation et la surveillance des réseaux locaux de type Ethernet. Les TP1 et TP2 sont une introduction au câblage. Le TP3 aborde l'architecture et les performances des réseaux Ethernet à travers la simulation, avec comme objectif de vous faire découvrir les architectures simples que vous pourrez rencontrer et l'influence de choix simples sur la performance du réseau. Les TP4 à TP7 vous introduiront la surveillance de réseau via le logiciel Wireshark (TP4 et TP5), l'outil RMON des switchs (TP6) et le module Netflow des routeurs (TP7). Ces TPs regroupent les connaissances de bases que doit avoir un administrateur réseau.

Déroulement

De manière à permettre à tous les TP de se faire sans dupliquer le matériel inutilement, tout en permettant de faire les TP dans un ordre logique pour chaque étudiant, l'organisation des TPs se fait selon le tableau ci-dessous, avec chaque colonne représentant le numéro de séance, et les lignes les numéros de binôme (attribués à la première séance).

	S1	**S2**	**S3**	**S4**	**S5**	**S6**	**S7**
Binôme 1	Rmon	Opnet	Wireshark 1	Wireshark 2	Câblage 2	Câblage 1	Netflow
Binôme 2	Netflow	Rmon	Opnet	Wireshark 1	Wireshark 2	Câblage 2	Câblage 1
Binôme 3	Câblage 1	Netflow	Rmon	Opnet	Wireshark 1	Wireshark 2	Câblage 2
Binôme 4	Câblage 2	Câblage 1	Netflow	Rmon	Opnet	Wireshark 1	Wireshark 2
Binôme 5	Wireshark 1	Câblage 2	Câblage 1	Netflow	Rmon	Opnet	Wireshark 2
Binôme 6	Wireshark 1	Wireshark 2	Câblage 2	Câblage 1	Netflow	Rmon	Opnet

Consignes à lire en début de chaque TP : Procédure et notation

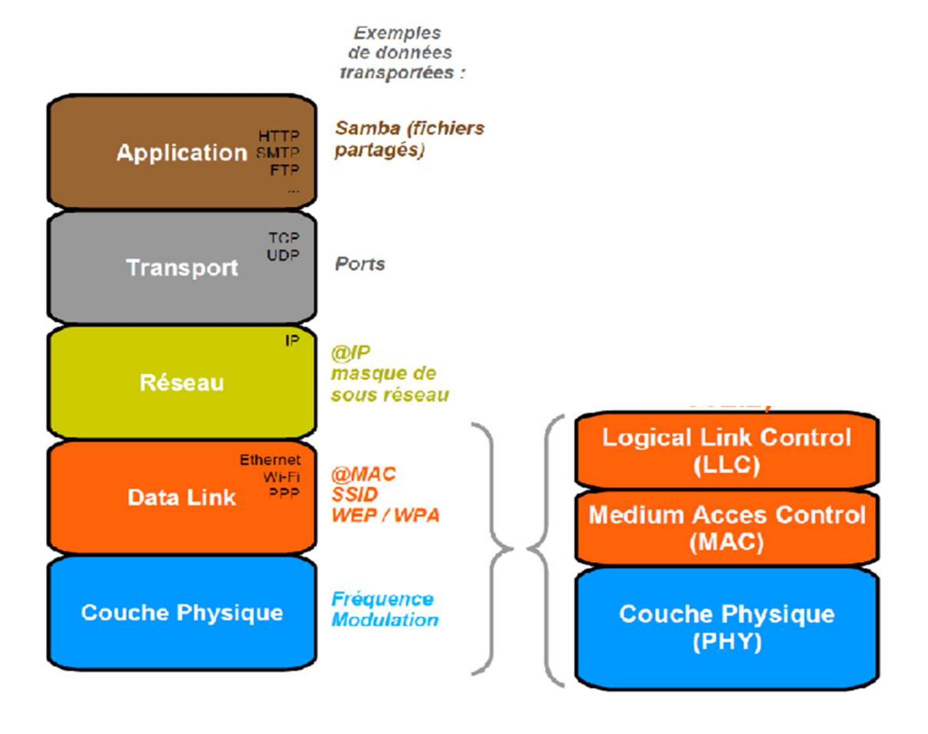
- **Notation** : La note de TP de R4 est constituée d'une note de contrôle continu = note rapport + interrogation en séance, et d'une note de DS de TP (en dernière semaine). Vous rendez un rapport par binôme à la fin de chaque séance de 3h.
- **Rapport** : A chaque question des sujets de TP qui ne sont pas des instructions de manipulation directe, vous devez répondre dans le rapport. Les réponses doivent toujours établir un lien avec le cours. Notamment, l'**interprétation en terme de couche OSI est capitale**. N'hésitez pas à faire des schémas (de topologie ou autre) dans le rapport pour qu'il gagne en clarté.
- **Notation en séance** : Si une partie de manipulation doit être validée, appelez l'enseignant pour la vérifier. Attention : toutes les explications données par l'enseignant doivent être clairement reproduites dans le rapport (pour montrer que vous avez bien compris).
- **Conseils** :
  - Il est évident que vous augmenterez vos chances de comprendre rapidement l'enjeu du TP et la configuration (et donc d'avoir une bonne note) en lisant l'énoncé du TP avant de venir en séance.
  - Devant une installation (notamment pour les TP de câblage), il faut comprendre cette installation et ne pas la considérer comme une boîte noire. N'hésitez pas à vous contorsionner pour voir les branchements. N'hésitez donc pas à regarder de partout. En revanche, **ne touchez surtout pas ce qui n'est pas sensé être manipulé par vous** ! (Les dégradations sont rapides avec le nombre d'élèves.)
  - Lorsqu'on vous demande de tester une connexion, ne vous précipitez pas sur un

navigateur web. Ayez conscience des mécanismes sous-jacents du réseau que vous avez appris en cours cette année : vous savez que la connexion au réseau local peut fonctionner sans que vous soyez relié à l'extérieur ou que vous ayez le droit de sortir du réseau local. Un test de connexion se fait donc sur le réseau local, par exemple par un ping vers le serveur de la salle (cf configuration de la salle ci-dessous).

- Vous devez venir en TP avec vos cours de réseau (R1, R2, R3, et R4). Dans tous les TP vous avez un accès web. Vous pouvez donc vous munir des versions électroniques des cours ou y accéder en ligne.
- N'hésitez pas à chercher des informations en autonomie sur le web. NB: tout copier-coller de wikipedia sera détecté et sanctionné.
- Les TP ne peuvent se faire indépendamment du cours, ils sont son application. Vous ne pourrez donc pas profiter (et accessoirement avoir une bonne note) des TP si vous venez en séances sans connaître votre cours.
- Les couches OSI doivent être parfaitement comprises et apprises. Un rappel ci-dessous.

Au début des années 1970, lorsque s'est posé le problème de faire communiquer 2 machines au travers d'un réseau, ce gros problème a été divisé en plusieurs sous-problèmes. Cette normalisation est le modèle OSI. Une couche du modèle OSI correspond donc à un sous-problème. Un protocole « appartient » à une couche s'il résout ce sous-problème. Un protocole correspond donc à un traitement effectué. Ce traitement est implémenté dans différents composants du réseau. Dans votre machine, où les traitement de toutes les couches sont implémentés, vous devez savoir où chacun l'est :

Couche	***Problème***	***Implémenté dans***	***Exemple de protocole***
Application	Communication machine/utilisateur	Logiciel	http, ftp, ssh, ...
Transport	Faire communiquer 2 machines entre elles indépendamment de ce qui se passe sur le réseau	OS	TCP, UDP
Réseau	Trouver le chemin entre les 2 machines (la suite d'équipements intermédiaires à traverser)	OS	IP
Liaison de données	Gérer l'accès au medium (câble, sans-fil, fibre, …), comme accès multiple, correction d'erreur, etc.	Carte réseau	Ethernet, WiFi, …
Physique	Assurer la traduction bit/ondes électromagnétiques	Carte réseau	Ethernet, WiFi, ...

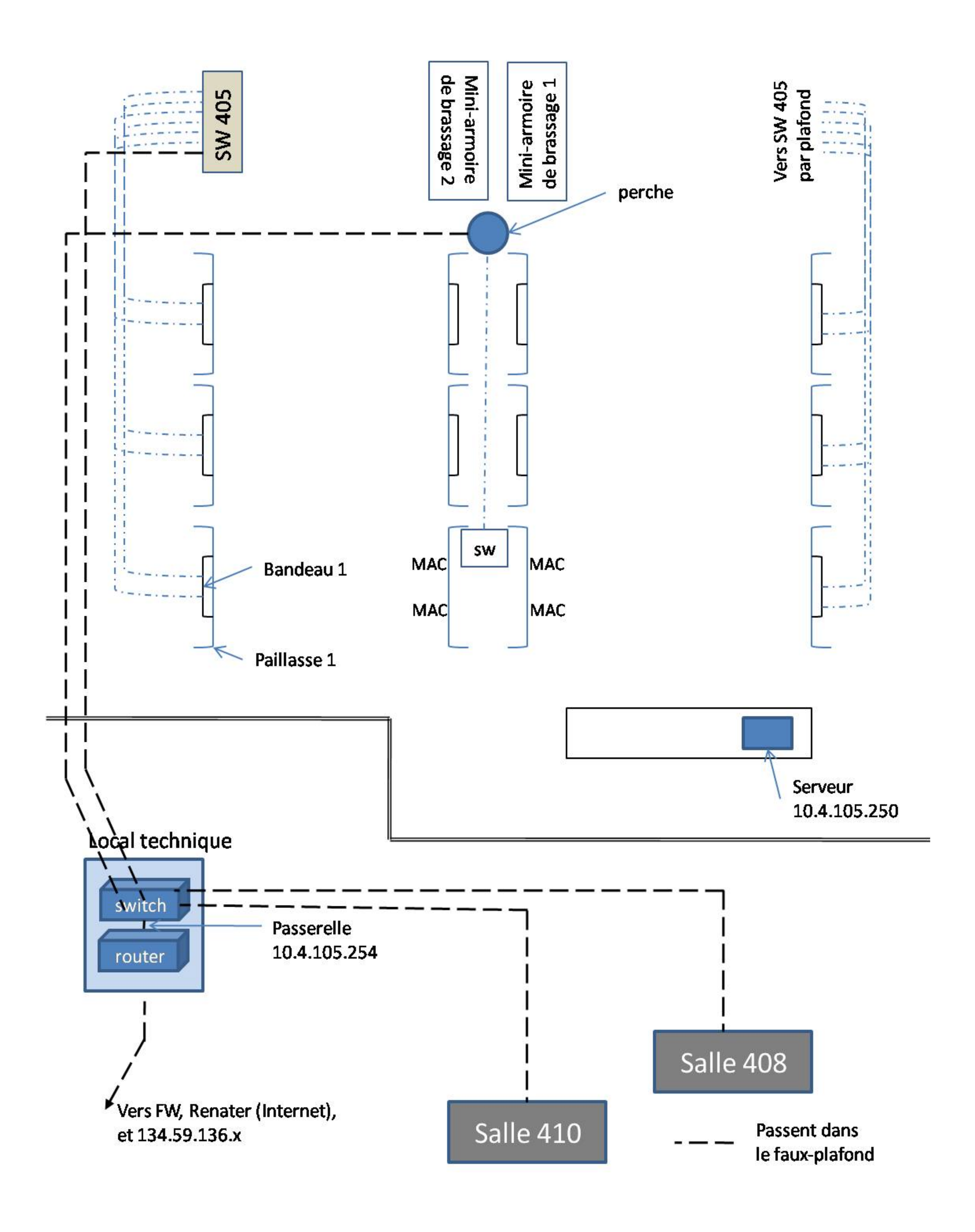


Configuration réseau de la salle

La description suivante fait référence au schéma de la page suivante.

Chaque salle du 4ème étage du bâtiment RT correspond à un réseau local particulier, dont l'adresse réseau est 10.4.1x.0 /24 . Le x vaut 05, 08 ou autre selon qu'on est en 405, 408. Dans notre cas, le réseau local est donc 10.4.105.0/24. Chaque réseau local correspond en fait à un VLAN (Virtual LAN) : ceci signifie que tous ces réseaux sont en fait reliés à un même switch, situé dans le local entre la salle 404 et le bureau 401. Ce switch effectue une segmentation en différents réseaux selon ses ports. Ce switch dispose également d'une connexion vers l'extérieur, notamment vers le réseau de l'IUT RT qui est en 134.59.139.x. Cela signifie donc que toutes (ou presque) les prises murales de la salle 405, situées sur les perches sont reliées par des câbles partant dans le faux plafond au switch de l'autre côté du couloir.
Sur le réseau 10.4.105.x, se trouvent 2 machines très importantes:

- la **passerelle** du réseau vers l'extérieur, c'est-à-dire le routeur dont un port est connecté au réseau local 10.4.105.x, et qui permet d'assurer le lien vers les autres réseaux. L'adresse de la passerelle (c'est-à-dire l'adresse IP de l'interface de ce routeur pour ce port) est **10.4.105.254**. Le routeur ne se trouve pas dans la salle 404.
- le **serveur** de la salle 405, qui est la machine du bureau enseignant, non accessible aux étudiants. Ce serveur est un serveur DNS, un serveur DHCP, un serveur mail et un serveur d'impression. Son adresse est **10.4.105.250**. Pour testez vos connexions, vous pourrez faire des ping vers ce serveur.


SW 405
Mini-armoire de brassage 2
Mini-armoire de brassage 1
Vers SW 405 par plafond
perche
sw
MAC
MAC
MAC
MAC
Bandeau 1
Paillasse 1
Serveur
10.4.105.250
Local technique
switch
router
Passerelle
10.4.105.254
Vers FW, Renater (Internet), et 134.59.136.x
Salle 408
Salle 410
Passent dans le faux-plafond

Mise en garde : pour s'y retrouver dans les câbles apparents

La salle 405 a 2 usages et 2 aspects (contrairement à l'an dernier où seul le premier était présent). C'est à la fois :

1. une salle d'utilisateurs de réseau, salle que vous devez administrer en tant qu'admin réseau (et système),
2. une salle d'expérimentation qui accueille les LP et les 2èmes années toute l'année.

Ces 2 utilisations correspondent à 2 ensembles d'équipements distincts :

1. Pour l'usage 1 :
   - les prises Ethernet murales sur lesquels les usagers « normaux » viennent brancher leurs ordinateurs : ce type de prise se trouve uniquement sur la paillasse du fond pour les TP1 et TP2 de câblage,
   - la perche, collectant les câbles venant des prises murales pour les faire partir dans le faux plafond jusqu'au switch situé dans la salle de brassage (porte sans poignée à côté de la salle 404).

2. Pour l'usage 2 :
   - le réseau expérimental est constitué de l'ensemble des équipements reliés aux câbles réseau blancs apparents qui ne passent pas dans le faux-plafond
   - les bandeaux au dessus de chaque paillasse rassemblent à la fois les câbles venant des PC (2 interfaces réseau par PC, carte TP est eth0 - à ne pas utiliser, carte IUT est eth1 - à utiliser), et les accès réseau : SW405 et Baie allant vers le switch SW405 (dans l'armoire au fond à gauche de la salle).

Le réseau expérimental est déployé pour avoir le maximum de flexibilité dans les configurations réseau pour différents TP (surtout LP), et vous devez savoir l'utiliser. Mais il est impératif que vous ayez conscience que la configuration normale d'une salle (ou bureaux, étage, bâtiment) utilisée par des usagers recherchant un simple accès réseau, est celle décrite pour l'usage 1. C'est celle dont vous aurez à vous occuper en tant qu'admin réseau/système.

Configuration système de la salle

Tous les TPs, sauf indication contraire, se feront sur VM Debian 6 que vous créerez en début de TP sur votre compte. Les exceptions sont :
TP1 : Machine physique 1 en Windows XP (compte rt, pas de mdp) et VMs Pour_TPR4 sur les autres, dans le compte rt
TP 3 : VM Windows XP Pour_TPR4_Opnet
TP6 : Machine Windows XP PourTP6_R4

TP 1 - Câblage : équipements d'interconnexion et segmentation

Introduction

L'objectif est de se familiariser avec les techniques de câblage réseau, les équipements d'interconnexion et les principes de segmentation d'un réseau. Après avoir étudié le réseau de la salle de TP (cf. début du fascicule de TP), vous devrez mettre sur le réseau l'ordinateur puis sécuriser ce réseau en segmentant celui-ci avec un switch.

Les ensembles de prises dans l'armoire sont des modules de raccordement de la gamme RCP (raccordements cuivre) utilisés à des points de concentration, comme dans un répartiteur général, sous répartiteur, point de consolidation, etc. Leur technologie leur offre la possibilité de supporter l'ensemble des applications les plus couramment utilisées telle que la voix, la donnée et l'image (VDI), utilisant généralement des câbles de catégorie 6. Les interconnexion sont ainsi plus fiables que des RJ45, engendrant moins d'erreurs, et plus pratiques à administrer.

Des câbles bleus sont à votre disposition en haut de l'armoire pour effectuer toutes les connexions demandées dans la suite. Ce sont des câbles Ethernet avec connecteurs CBE s'enfichant dans les prises RCP. Tout est donc équivalent à du RJ45, mais pas sous le format jack RJ45.

NB: Les câbles bleus sont à manier avec précaution, attention lors du branchement, il y a des détrompeurs sur les câbles, ne forcez pas ! Tous les câbles sont droits (vous aurez à expliquer pourquoi cela suffit dans les questions suivantes).

EN AUCUN CAS VOUS NE DEVEZ TOUCHER AUX CONNEXIONS DES PC AUX PRISES DE LA TABLE

Questions

Partie 0 : Prise en main

Prenez le temps d'identifier la configuration pour ce TP:

- identifier quels sont les équipements d'interconnexion présents dans l'armoire
- repérer toutes les étiquettes dans l'armoire, indiquant la façon dont est faite la partie de câblage non facilement visible
- identifier chacun des ensembles de prises de l'armoire : quels sont les connexions avec les équipements précédents ? Avec les PC ?
- identifier les alimentations en réseaux sur la perche située derrière l'armoire de brassage
- identifier leurs arrivées au niveau de l'armoire

Partie 1 : Premiers tests avec le hub

Dans un premier temps, on veut établir la connexion depuis la perche vers le Hub :

- quel type de câble (droit ou croisé) faudrait-il normalement utiliser, connaissant la topologie du réseau de la salle (donnée en début du fascicule de TP) ?
- Pourquoi ? Rappeler les définitions et implications des ensembles MDI/MDIX clairement dans le rapport.
- En observant le hub, indiquer comment un câble droit peut convenir.

- Établir la connexion perche / hub.
- Démarrez le PC1 (le plus proche de l'armoire) sous Windows.
- Connectez PC1 sur le hub via les points d'accès appropriés.

- Vérifiez la réussite de votre manipulation (cf. début du fascicule: protocole de test d'une connexion).
- Comment récupérer l'adresse IP et l'adresse MAC de votre machine : En Windows ? En Linux ?
- Comment déterminer l'adresse MAC d'un équipement à partir de son adresse IP ? Décrivez pour cela l'envoi d'un ping avec le mécanisme ARP en établissant un lien précis avec les couches OSI (voir début de fascicule de TP).
- Relevez les adresses IP et MAC de PC1, ainsi que serveur et passerelle dont vous connaissez les adresses en connaissant la configuration du réseau de la salle.

Partie 2 : Premiers tests avec le switch

Alimentez le switch directement en Internet en reliant le câble venant de la perche sur le switch (en port 9 par exemple) et reliez les 4 ordinateurs à votre disposition sur les ports 1 à 4 du switch.

- Vérifiez la réussite de votre manipulation sur chacun. Pensez à vérifier la configuration de l'interface réseau, et désactiver et ré-activer les interfaces si les premiers tests n'aboutissent pas.

Partie 3 : Installation du switch et accès en mode console

Munissez-vous du guide d'utilisation du switch (posé à votre portée) pour comprendre et répondre aux questions suivantes.

Trois interfaces sont disponibles pour le switch. Le mode *console* permet de se brancher directement sur le switch par port série et d'obtenir une émulation de type VT-100. Le mode *telnet* permet d'accéder au même genre de menu de configuration, mais en utilisant le protocole Telnet au dessus d'une connexion TCP/IP. Enfin, le mode *interface de navigateur Web* (ou *Web browser interface*) permet d'accéder à la configuration et supervision du switch via une connexion HTTP (pages html). Néanmoins, ces deux derniers modes d'accès nécessitent une connexion TCP/IP, et requièrent donc que le switch dispose d'une adresse IP, ce qui n'est pas le cas s'il n'a pas été configuré pour. Il va donc falloir utiliser la connexion série pour ensuite pour avoir accéder au switch par le réseau. Le port série du switch est relié au port série du PC qui jouxte l'armoire.

- D'abord, pour assurer une configuration stable, faire un *reboot d'usine* (cf. notice d'utilisation du switch).
- Dans un terminal du PC, lancer le communicateur série `hyperterminal`.
- Configurez une nouvelle connexion série vers le switch. Les paramètres de cette connexion doivent être trouvés dans la notice du switch. Indiquez-les dans votre rapport.
- Taper deux fois sur la touche `Entrée`. Si tout se passe bien, vous entrez alors dans le menu de configuration du switch en mode console.
- Lorsque hyperterminal établit la connexion avec le switch en mode console, une page d'accueil apparaît puis un prompt CLI. A ce prompt, tapez « menu ».

- Quels sont les avantages et inconvénients de pouvoir supprimer les mots de passe par simple pression d'un bouton à l'avant du switch ?

Note (mots de passe) : Dans le cas où un mot de passe serait requis pour entrer dans le mode console, il peut être effacé par une pression sur le bouton `Clear` à l'avant du switch. Cette opération réinitialise toutes les protections par mot de passe de la configuration du switch.

Note (retour à la configuration d'usine) : Le retour à la configuration « d'usine » se fait par une pression simultanée sur les boutons `Reset` et `Clear`, en gardant appuyé ce dernier jusqu'à ce que le voyant *Self Test* commence à clignoter.
On peut également, dans le mode CLI , taper la commande `erase startup-config` pour faire rebooter le switch dans sa configuration d'usine.

Partie 4: Attribution d'une adresse IP

Dès que le switch disposera d'une adresse IP, l'accès au mode console sera également accessible par un simple `telnet`. Par défaut, le switch est configuré pour acquérir une adresse IP par DHCP/Bootp. Il peut également être forcé en mode manuel pour recevoir une adresse IP spécifique.

1. Depuis le menu principal, aller dans `2. Switch Management Access Configuration` puis `1. IP Configuration`, faire ensuite l'action `Edit`, se déplacer sur `IP Config [DHCP/Bootp]:` et appuyer sur la touche espace pour positionner `Manual`.
2. Donner ensuite l'adresse IP `10.4.105.242` avec le masque de réseau `255.255.255.0`. La passerelle sera en `10.4.105.254.` Faire alors l'action `Save`: le switch dispose d'une adresse IP.
3. Dans le menu `3. Switch Configuration` puis `1. System Information` pour les 2424M, il est possible de donner un nom au switch (pour faciliter son identification: par exemple, *SwitchN* comme dans la figure plus bas).

- Quel est la couche OSI concernée par le travail d'un switch ?
- Quelle est la couche OSI correspondant à IP ?
- Expliquer alors pourquoi nous attribuons une adresse IP à nos switchs.
- A quoi faut-il faire attention lors de l'attribution de l'adresse IP au switch ?

Partie 5 : Accès au switch sans liaison série

Puisque le switch dispose d'une adresse IP, il est possible de s'y connecter en mode console par un `telnet` ou bien en mode navigateur par HTTP. Néanmoins, soyez conscients du fait que seul le mode console (liaison série) ne *pollue* pas les observations que l'on peut faire sur le trafic: les modes telnet ou Web étant supportés par TCP/IP, et donc transportés par Ethernet, ils génèrent des trames Ethernet qui peuvent rendre confuses les observations que vous devez réaliser dans la suite de ce TP.

1. De PC1, tentez un `ping` vers l'adresse IP que vous avez donnée au switch.
2. Une fois que le switch et le PC sont visibles l'un de l'autre, accédez au switch en mode telnet.
3. Regarder ses tables d'adressage ainsi que l'état de ses ports.
4. Qu'est-ce qu'une table d'adressage ?
5. Faire la même chose en accédant au switch via l'interface Web par l'URL

`http://10.4.105.242` et regardez les différents onglets (constatez avec `wireshark` les répercutions sur le trafic).

- Décrivez les avantages et inconvénients de chacun des modes d'accès aux switchs (console, telnet et Web).
- Pouvez-vous voir la table d'adressage et l'état des ports du switch dans tous les modes ?
- A quoi correspond la table d'adressage ?

Partie 6: Etude de l'établissement de la table ARP d'une machine

Pour étudier la commutation Ethernet, nous utilisons un outil relativement simple: `ping`. Néanmoins, même s'il est simple et permet de générer des trames Ethernet, cet outil travaille au niveau 3 des couches OSI, c'est-à-dire au niveau IP (le message ICMP echo request est encapsulé par IP).

L'état de la table ARP peut être consulté sur A avec la commande `arp -a`. Il ne faut pas confondre cette table ARP (@MAC<=>@IP) avec la table des adresses (@MAC<=>n°port) du switch.

Etude de l'établissement de la table ARP d'un PC :

0. Connectez-vous sur le compte rt/rt sur PC2, et lancez la VM PourTP1_R4. De même sur les 2 MAC du bout. Après avoir établi les bonnes connexions dans la mini-armoire de brassage, vérifiez que les 4 machines (VM pour PC2 à 4 et Windows natif pour PC1) ont leur interfaces correctement configurées et fonctionnelles.

1. Sur PC1, connectez-vous au switch en mode série et affichez la table d'adressage.
2. Sur PC2 et PC4, lancez wireshark (le logiciel Wireshark permet d'observer le trafic dans un mode graphique).
3. Sur PC3, effacez le contenu de la table arp en faisant arp -a et en faisant arp -d @IP pour l'adresses IP de PC4 si elle s'y trouve.
4. Lancez une capture sur PC2 et PC4.
5. De PC3, faire un ping vers PC4.
6. Des paquets visibles (à analyser) sur PC2 et PC4, que déduisez-vous comme mécanisme d'établissement de la table ARP d'un PC ?

Partie 7: Établissement de la table d'adressage du switch

7. Sur PC1, connectez-vous au switch en mode série et affichez la table d'adressage.
8. Sur PC2, lancez wireshark.
9. Débranchez et rebranchez les ports des PC3 et PC4 sur le switch, et vérifier que ces entrées disparaissent de la table d'adressage.
10. Lancez une capture sur PC2.
11. De PC3, faire un ping vers PC4. Simultanément regardez l'évolution de la table d'adressage du switch (sur PC1).
12. Des paquets visibles (à analyser) sur PC2, que déduisez-vous comme mécanisme

d'établissement de la table d'adressage d'un switch ?

Partie 7 : Port Monitoring

Pour surveiller le trafic, il est possible de renvoyer sur un port précis du switch la totalité du trafic qui circule normalement sur un ou plusieurs autres ports. Cela peut être particulièrement intéressant pour surveiller l'activité d'un ensemble de ports.

1. Configurez le switch de façon à ce que le port 4 du switch reçoive les trafics des ports 2 et 3 du switch (4 est dit *moniteur*). Ceci est réalisé en interne, sans câble extérieur. Pour cela, dans le menu principal, faire `Switch Configuration` puis `Network Monitoring Port` et placer `Monitoring Enabled` à `Yes`. Spécifier ensuite qui est moniteur et qui est monitoré.
2. Observer depuis le PC4 (avec `wireshark`), l'activité sur les ports monitorés au repos et lors de ping entre différentes machines : que constatez-vous ?

Partie 8 : Domaines de diffusion

Dans cette partie, vous allez configurer deux VLAN par port, un « rouge » et un « vert ». Chaque VLAN comprendra deux machines.

1. Vérifier l'état de la table d'adressage du switch et regarder le trafic sur chacune des interfaces des PC (avec `wireshark`), en particulier lors de ping entre les différents PC.
2. En l'absence de toute information dans la table d'adressage du switch, vérifier que tous les PC voient les messages ICMP générés par un ping, y compris les trames unicast.
3. Vérifiez que lorsque le switch dispose de l'association, seules les deux machines concernées par le ping voient le trafic. Que se passe-t-il alors si la machine réalisant le ping n'a plus rien dans sa table ARP ?

VLANs non taggés

On désire maintenant que le trafic entre PC1 et PC4 soit complètement différencié du trafic entre PC2 et PC3, c'est à dire qu'aucun échange ni observation ne puisse avoir lieu entre ces deux *réseaux locaux virtuels*. Pour cela, on peut créer deux VLANs distincts: le VLAN *rouge* pour PC1 et PC4 et le VLAN *vert* pour PC2 et PC3. Ce sont des VLANs *par port*, compatibles avec la norme IEEE 802.1Q. En l'absence de toute configuration, les switchs considèrent que tous les ports font partie du même VLAN par défaut.

1. Autoriser les VLANs
   Dans le menu principal d'administration du switch, aller dans `Switch Configuration`, puis `VLAN Menu` et finalement `VLAN Support` , vérifier que le support est OK.
2. Définir les VLANs
   Ensuite, dans le menu VLAN, faire `VLAN Names` et ajouter les deux VLANs, le rouge et le vert. Par défaut, tous les ports du switch appartiennent au `DEFAULT_VLAN` qui a `1` pour numéro (`VLAN ID`). Il est important de **ne pas modifier ce VLAN par défaut**. Donner des VLAN ID différents pour les VLAN créés. Par exemple, **`20`** pour le VLAN **rouge** et **`30`** pour le VLAN **vert**.
3. Assigner les ports aux VLANs
   Dans le menu VLAN, faire `VLAN Port Assignment`. Chaque port est alors proposé pour chaque VLAN (défaut, rouge, vert), et *taggé* ou non : utiliser les VLAN rouge et vert *sans les tagger*. Associer le rouge aux ports reliant le PC1 et le PC4 et le vert aux ports

reliant le PC2 et le PC3.

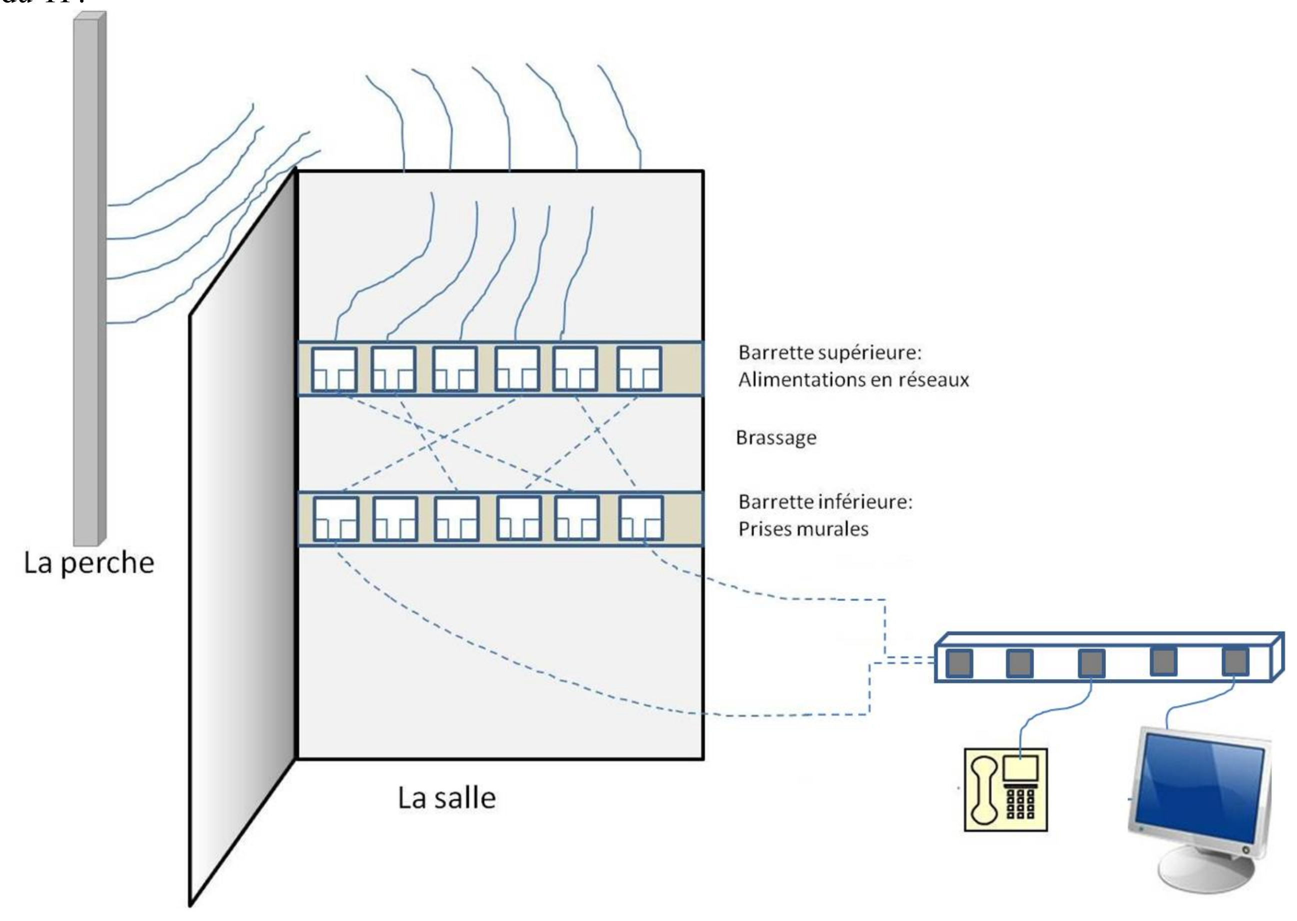
4. Tester alors la communication entre les différents PC et regarder l'activité du trafic sur les différentes interfaces, comme dans l'exercice 1. Expliquer ce qui se passe.
5. Vérifier en particulier si les broadcasts ARP générés par un ping d'une machine sur un VLAN atteignent ou non les machines de l'autre VLAN.
6. Donnez un accès internet au VLAN rouge. Que faudrait-il faire pour avoir un accès internet sur les deux VLANs ?

Remettez tout à son état initial

TP 2 - Câblage : : fabrication de câbles et brassage

Description

Ce TP de câblage/brassage consiste principalement à fabriquer un câble et à installer une « mini-salle » avec une « mini-armoire de brassage ».
Le schéma de l'installation que vous avez devant vous est représenté sur la figure suivante. Les connexions (notamment en pointillés) ont uniquement un but d'illustration, et ne correspondent pas exactement aux numéros des prises que l'on vous demande d'analyser et trouver dans les questions du TP.



L'armoire de brassage que vous avez devant vous représente à la fois la salle pour laquelle vous allez devoir réaliser le câblage (donc les prises réseau aux murs de la salle), ainsi que l'armoire de brassage à laquelle ces prises murales vont converger et qui va vous permettre de donner aux utilisateurs de la salle l'accès aux réseaux que vous voulez, opération appelée *brassage*.

Dans l'état initial, 5 prises d'alimentation (i.e., venant de l'extérieur de la salle) sont câblées dans l'armoire de brassage et une prise est câblée vers les prises murales de la mini-salle.

- Dans une première étape, vous allez réaliser un câble Ethernet avec connecteurs RJ45, et en profiter pour vous remémorer sa structure et la fonction de chaque fil.
- Dans une deuxième étape, vous devez identifier les câbles entrant dans l'armoire et les connecter sur la perche selon les instructions.

- Ensuite, vous devez connecter les prises de « sortie » de l'armoire de brassage vers les prises murales selon les instructions données.
- Enfin, vous devez tester le câblage par le test de connectivité via le téléphone et l'ordinateur (ifconfig et ping).
- Finalement, comprendre la composition des trames et la relation avec la durée des signaux électriques.

NB: les 2 PC à droite de l'armoire sont à votre disposition. Utilisez celui de droite pour l'accès Internet. **Ne débranchez jamais la prise ethernet la plus haute sur la barrette, ainsi que celle utilisée par l'autre mini-armoire du TP1.**

Questions

1. Fabriquer un câble RJ45 droit selon la norme TIA/EIA-568B:
    - rappeler d'abord le code couleur et les **fonctions des différents fils** dans le rapport (voir http://www.bytepile.com/includes/cable_categories_main_table_color_codes.php)
    - repérer comment numéroter les broches (*pins*) sur le connecteur RJ45
    - Lisez entièrement la page : http://etienne.durup.free.fr/cablage/jecable2.htm, afin de comprendre comment est fait un câble, et ensuite en construire un.
    - Une fois les étapes précédentes FAITES, appelez l'enseignant pour qu'il vous donne le matériel pour réaliser un câble droit (une extrémité faite par chaque membre du binôme).
    - Une fois réalisé, vérifier votre câble par le testeur de connectivité à votre disposition.
    - Faites vérifier votre câble par l'enseignant.

2. Identifier les réseaux auxquels sont reliées les prises sur la perche. Les indiquer dans le rapport sous la forme « numéro de prise → adresse de réseau ».
    - Détaillez le principe d'une prise double : comment peut-on avoir 2 réseaux sur le même connecteur RJ45 ?
    - Pour la prise double, déterminez à quelles paires est attribué chaque réseau (en sachant que le premier réseau mentionné sur l'étiquette est attribué aux broches principales, c'est-à-dire toujours utilisées).

3. Déterminer quels câbles (identifiés par leurs numéros au stylo) d'alimentation de la mini-armoire doivent être liés à quelles prises de la perche si on désire pouvoir connecter les différentes prises murales (une seule prise murale est câblée pour l'exemple) aux:
    - soit réseau 10.4.105.x/24 soit réseau 10.4.110.x/24 (à l'aide de la prise double)
    - et réseau téléphonique

    et effectuez ces branchements.

4. Est-il possible d'avoir une prise double avec au moins un des 2 réseaux en Gigabit Ethernet ?

5. Sachant qu'au bout de la prise du réseau 10.4.105.x sur la perche se trouve un commutateur (cf. Configuration du réseau de la salle en page 3) :
    - devrait-on avoir un câble droit ou croisé pour la connexion allant du switch de la paillasse des MAC où vous êtes à la prise murale reliée à la prise du réseau 10.4.105.x ? Rappelez clairement les ensembles MDI/MDIX dans votre réponse.
    - Trouver une solution si l'on veut réaliser cette connexion avec le câble qui ne convient pas a priori, en réfléchissant à tous les éléments traversés par votre câble.

6. Testez (uniquement écoute de la tonalité, ne le faites pas sonner, ça vous enlèverait des points) la connexion avec le téléphone, qui sera branché à une prise murale de la barrette inférieure de l'armoire.

7.0. Connectez-vous sur votre compte (chaque étudiant du binôme sur un PC différent, sur son compte perso). Dans un terminal, exécutez

```
createvm-gm VMTP2 Debian6admin-201303.SATA.vdi eth1 100 SATA
```

Une fois la machine créée, regénérez son adresse MAC.
Logins et mdp habituels : rt/rt

7.1. Ensuite avec l'ordinateur, testez votre connexion au réseau 10.4.105.x.

8. Testez votre connexion au réseau 10.4.110.x en établissant les connexions adéquates, et en entrant les commandes :

```
ifconfig eth0 10.4.110.230 netmask 255.255.255.0 up
route add default gw 10.4.110.254
```

Faite un `route -n` et un `ifconfig eth0` pour vérifier que la configuration est effective.

Faites valider par l'enseignant.

9. On suppose dans la suite que la vitesse de notre réseau est de D=10 Mbit/s. Combien d'octets contient un paquet dont la durée d'émission est de T µs (donner la formule littérale)?

10. Repassez sur le réseau 10.4.105.x. Lancer Wireshark. Dans quels protocoles est encapsulé un message ICMP avant d'être émis dans une trame Ethernet ?

11. Indiquer la longueur du message ICMP *echo request*, la longueur de chaque entête, et la longueur totale de la trame, en octets ?

12. Les figure 1 et 2 représentent des trames Ethernet 10 Base T capturées sur un oscilloscope. Le préambule est une suite de 0 et de 1 alternés. Il permet à l'horloge du récepteur de se synchroniser sur celle de l'émetteur.
Calculer la durée du préambule en connaissant le débit D de transmission (donner la formule littérale), et donner la valeur numérique pour un réseau avec D=10Mbits/s.

Nombre d'octets :

Préambule	Adresse Destination	Adresse Source	Ether Type	Données	CRC
8	6	6	2	46 à 1500	4

Format de la trame Ethernet V2

13. Grâce à la réponse à la question 11, donnez la durée totale théorique d'une trame Ethernet encapsulant le message *ICMP echo request*.
Détaillez le calcul avec la longueur de chaque entête protocolaire et le débit D.

14. Donnez la commande pour lancer des pings, de façon à ce que les paquets envoyés soient d'une taille donnée en paramètre (vous pouvez vous aider de la commande `man ping`).

15. Lancer une série de pings avec une taille de paquet de 1472 octets, puis 1473 puis 3000; faites ces 3 captures successivement. Après chacune, observez les champs *IP id,* et les différents *flags* : à quoi correspondent-ils ? Quelle est la valeur du *segment offset* et pourquoi ?

16. Analysez le détails de IP et ICMP, pour comprendre la différence entre ce qu'il se passe pour 1472 et 1473. Notamment à quoi correspond 1518 ?

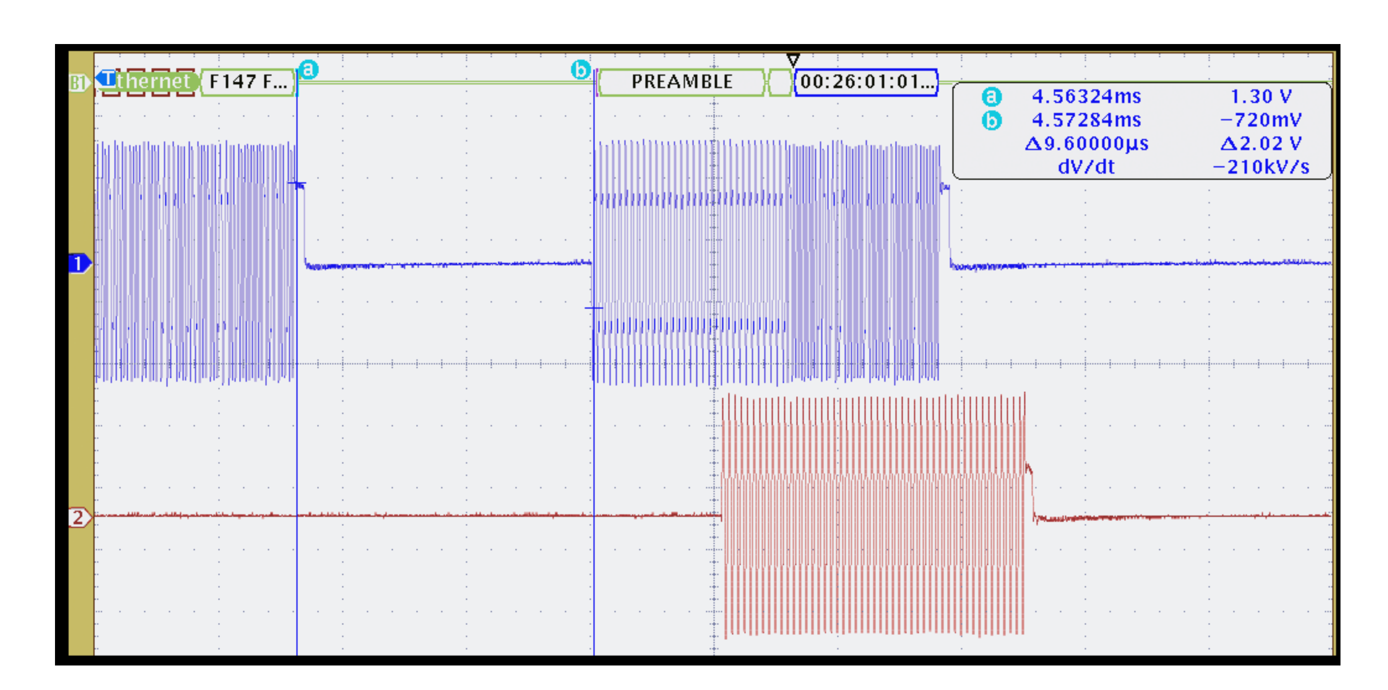


Figure 1 : Trames Ethernet en 10 Base T. 1 division = 4µs

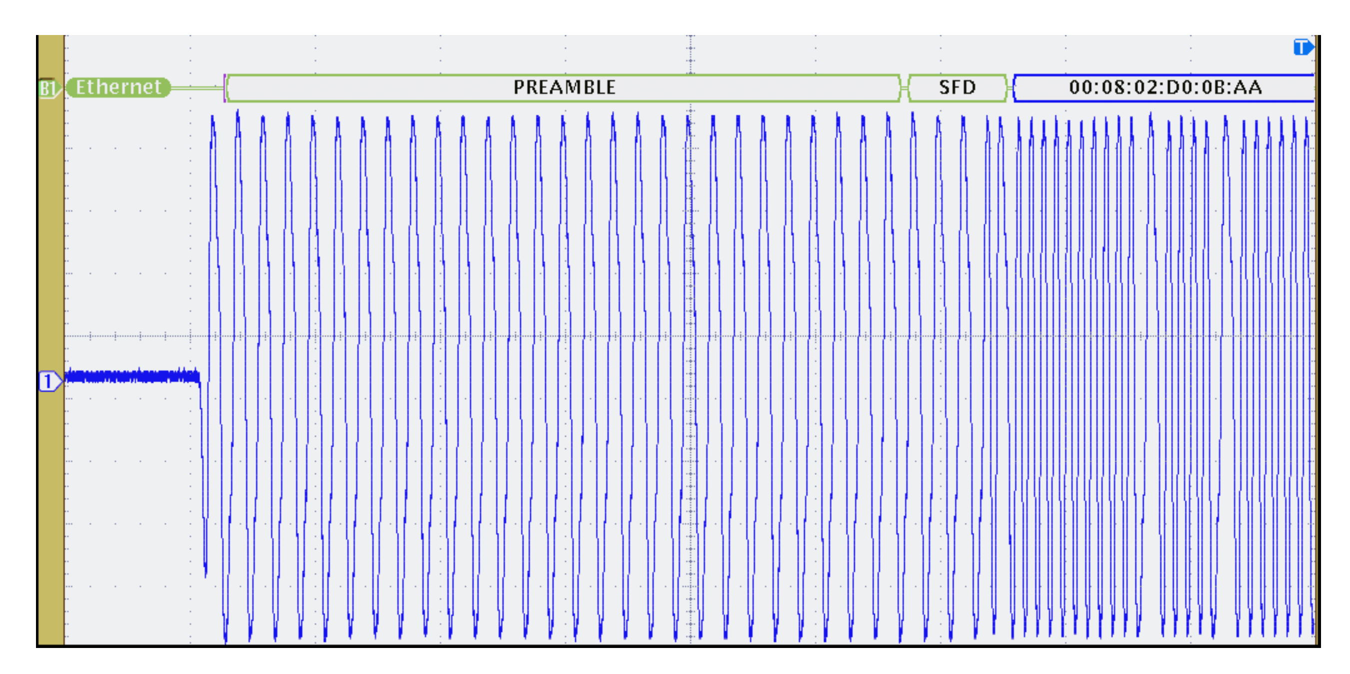


Figure 2 : Une partie d'une trame Ethernet en 10 Base T. 1 division = 1µs

TP 3 - Simulation de réseaux avec OPNET

Introduction

Opnet est un logiciel de simulation de réseau. Contrairement à Wireshark ou au switch avec RMON ou routeur avec Netflow, il ne permet non pas d'observer et analyser du trafic réel sur le réseau de la salle, mais de prévoir les performances d'un réseau « fictif » dont on lui fournit toutes les caractéristiques (topologie, équipements, types de trafic et charge).

Nous allons donc utiliser Opnet pour étudier et comprendre les performances d'un réseau local fonctionnant avec Ethernet dans différentes conditions, et notamment comprendre l'origine protocolaire des différences de performances si on utilise un switch ou un hub pour l'interconnexion.

Chaque étudiant se connecte sur une machine de la paillasse, sur le compte rt/rt, et lance la VM nommée PourTP3_R4_Opnet.

NB : Vous devez suivre les étapes de configuration pas à pas rigoureusement. Le logiciel ne permet pas facilement de revenir en arrière dans la configuration du réseau.
En plus des explications détaillées, le rapport devra contenir des reproduction à la main de l'allure des courbes avec quantités et unités en abscisse et ordonnée.

Étude d'un petit réseau

Dans cette partie, on souhaite comparer les performances de deux réseaux simples comprenant chacun un serveur et trois clients, mais reliés par un hub ou par un switch. Pour chaque réseau, on va définir trois scénarios différents (on utilisera des liens 10BaseT) :

1. les 3 clients ont une faible activité ;
2. les 3 clients ont une activité très importante qui risque de surcharger le réseau ;
3. les machines ont une activité très importante, deux à deux.

<u>Effectuez les étapes de configuration suivantes :</u>

1. Lancez IT guru et créez un nouveau projet tp3_petit_votre_nom
2. Créez un scénario : tp3_hub, avec un environnement *Office*, d'une dimension de 100m x 100m et la technologie Ethernet.
3. Faîtes glisser trois stations Ethernet (ethernet_wkstn), un serveur et un hub dans la fenêtre de construction du réseau. Connectez les éléments au hub via des liens Ethernet 10 Mbps.
4. Ouvrez le projet TP_profile, copier les nœud Application et Profile, collez les dans votre projet.
5. Appliquez le profile *web* aux stations (sélectionner toutes les stations, ouvrez la fenêtre d'attributs (clic droit), appliquez le trafic voulu dans la ligne *Application Supported Profiles.* Puis edit → ajoutez une ligne (Rows), n'oubliez pas de cochez *Apply changes to selected objects*.
6. Configurez le serveur en serveur « toutes applications » (ouvrez les attributs, ouvrez les applications, dans la fenêtre *Application Supported Services -> All*
7. Pour choisir le type de statistiques à observer, sous le menu *Simulation → Choose individual statistics*. Puis *Node statistics.* Pour cet exercice, on choisira les performances au niveau d'Ethernet : sélectionnez Ethernet.

8. Lancez la simulation, pour une durée de 30 minutes (*Simulation → Discrete event simulation*).
   Attention : il s'agit de simuler du trafic sur 30 min, mais simuler ce trafic et faire le calcul des performances ne prend que quelques secondes ! (le bip indique la fin de la simulation).

9. Dupliquez le scénario (*Scenario → Duplicate*), appelez le tp3_switch. Remplacez le hub par un switch (prendre le *ethernet16_switch*). Lancez la simulation pour une durée de 30 minutes.

Analyse des résultats :

10. Un fois les simulations terminées, allez dans *Results → View results* . Sélectionner un nœud correspondant à une station. Visualisez le délai au niveau Ethernet. Au niveau de la figure, sélectionnez *Overlaid statistics*, *average* et *All scenarios.* Cliquez enfin sur *Show.* Vous avez un figure que vous pouvez à présent analyser.
11. A quoi correspond le « délai au niveau Ethernet » exactement ?
12. Rappelez le fonctionnement d'un hub précisément : qu'advient-il d'une trame entrante ?
13. Rappeler le fonctionnement d'un switch précisément : qu'advient-il d'une trame entrante ? Décrire l'ensemble du processus de traitement au niveau du switch. (Rappelez-vous des tables d'adressage...)
14. Déduisez-en la raison pour laquelle vous observez ces performances en terme de délai.

Configuration :

15. Dans les deux scénarios, utilisez le profil d'application *haut débit* sur les stations, en veillant à ce que le champ *Application Supported Services* du serveur est toujours mis à *All services*. Dans les deux scénarios, appliquez un facteur multiplicatif de trafic de 10 (*Simulation → Configure Discrete Event Simulation →* Onglet *Global Attributes*, mettre l'attribut *Traffic Scaling Factor* à 10 et l'attribut *Traffic Scaling Mode* à *All Traffic*. Simulez sur trois minutes.

Analyse des résultats :

16. Comparez les performances et expliquez les différences (même manips qu'en question 10) :
    - Quel est le plus rapide (en terme de délai) dans ce contexte (hub ou switch) ?
    - Qu'est-ce qui a changé dans la configuration du réseau simulé pour obtenir ce changement ?
    - Expliquez le mécanisme CSMA/CD : définir l'acronyme et expliquez en détail à quoi ça sert et comment ça marche.
    - Visualiser les collisions (depuis le scénario hub). Que constatez-vous ?
    - En raisonnant sur le buffer de la couche liaison de données (sous-couche MAC) et sur les débits appliqués, expliquez l'allure de la courbe de délai (toujours au niveau d'une station) du switch et du hub (croissance au cours du temps pour le hub) ?

Configuration :

17. Ouvrez le projet TP_Trafic_spécifique. Dans ce projet, les lignes bleues représentent un trafic de 10 Mbps entre les paires d'équipements. Sélectionner toutes les métriques Ethernet dans *Individual Node Statistics* et faites les simulations sur 3 minutes pour chacun des scenarios switch et hub.

Analyse des résultats :

18. Pour chaque nœud, les quantités *load* et *traffic received* correspondent au trafic émis et reçu par le nœud, respectivement. Pour chaque nœud, afficher le trafic entrant et sortant (en bits/s par exemple) au niveau Ethernet et vérifier que tout le débit sortant d'un nœud se retrouve bien dans un autre.
19. Affichez 4 fenêtres avec le débit de trafic sortant (*load* en bits/s) pour chacun des 4 nœuds dans les 2 cas : dans chaque fenêtre doit apparaître 2 courbes, celle dans le cas du switch et celle dans le cas du hub.
20. Sachant que les câbles sont des 10BaseT, et que les cartes réseau permettent du 10Mb/s, que pouvez-vous dire sur la répartition du débit total par un hub et par un switch ? Raisonnez sur les valeurs précises et indiquez votre calcul.
21. Pour chaque nœud, afficher ensuite *load* en packet/s et *traffic received* en packet/s
22. Que constatez-vous pour la proportion de trafic émis par rapport au trafic reçu pour chaque nœud ?
23. De quel type d'échange s'agit-il à votre avis, et pourquoi ?
24. Identifier les émetteurs et récepteurs de données utilisateur.

TP 4 - Wireshark : analyse de trames Ethernet, ICMP et ARP

Introduction

Wireshark est un logiciel d'analyse de trafic. Il permet de contrôler la carte réseau de la machine sur laquelle il tourne, récupère les trames vu par la carte réseau et permet une analyse aisée des paquets. Le but de ce TP est d'abord de comprendre précisément la structure et la hiérarchie sous laquelle Wireshark présente les informations de trafic, en identifiant le rapport avec la normalisation du fonctionnement d'un réseau (notamment les différentes couches OSI). Une étude d'ICMP et d'Ethernet sera ensuite réalisée.

Ce logiciel est gratuit et existe sous Linux et Windows. N'hésitez pas à l'installer sur vos machines personnelles et à regarder ce qui se passe sur votre réseau en dehors des cours.

Ce TP se fait grâce à wireshark, qui est installé sur les machines virtuelles Linux.
Connectez-vous sur votre compte (chaque étudiant du binôme sur un PC différent, sur son compte perso). Dans un terminal, exécutez
`createvm-gm VMTP4 Debian6admin-201303.SATA.vdi eth1 100 SATA`
Une fois la machine créée, regénérez son adresse MAC.
Logins et mdp habituels : rt/rt
Passer en root en tapant: *su*, password: *rt*. Tapez *wireshark &* pour lancer le logiciel.
Comme pour les autres TP, toutes les étapes sont à faire dans l'ordre.

Prise en main

- Dans l'onglet Capture, cliquez sur Options. Sélectionnez l'interface sur laquelle la capture doit être réalisée (eth0 en général), décochez « *promiscious mode* » et les différentes « *name resolutions* ». Cliquez sur Ok. La capture est lancée.
- Connectez vous sur http://kheops.unice.fr. Une fois cette page chargée, arrêtez la capture.

Nous allons à présent procéder à une analyse structurée, « du plus général au plus détaillé », de la façon dont Wireshark représente le trafic. Il est INDISPENSABLE de lire le rappel sur les couches OSI en début de fascicule.

1. Vous voyez que la fenêtre principale de Wireshark, où apparaît le résultat de la capture, est divisée en 3 sous-fenêtres. Cliquez sur une ligne. Donner la signification d'une ligne dans la première sous-fenêtre (celle du haut). Attention: on veut que vous identifiez l'entité générale représentée par une telle ligne, et non les détails de cette ligne.

2. Structure générale de la 2ème sous-fenêtre: que représente chaque ligne de cette sous fenêtre ? Attention, on ne veut pas des noms de protocoles spécifiques, mais que vous explicitiez la relation entre la 2ème sous-fenêtre et les couches OSI. Votre réponse doit être valable quelque soit le paquet sur lequel vous cliquez. Détaillez votre réponse.

3. 3ème sous-fenêtre : à quel alphabet appartiennent les symboles affichés dans cette fenêtre ? Que représentent-ils ? Cliquez sur une ligne de la 2ème sous-fenêtre. Que se passe t-il dans la 3ème ? A quoi cela correspond t-il ?

4. Identifiez à quoi correspondent exactement les parties surlignées pour chaque ligne de la 2ème sous-fenêtre dans la 3ème sous-fenêtre.

5. Quel processus général relatif au fonctionnement du réseau la 3ème sous-fenêtre vous permet-elle de voir ?

6. A quoi correspond le protocole indiqué dans l'avant-dernière colonne de la 1ère sous-fenêtre ?

Maintenant que la structure générale de représentation du trafic est identifiée, et que vous avez pu faire le lien direct avec votre cours réseau,. affichez le premier paquet « HTTP GET ».

6. Listez les protocoles utilisés sur le réseau. Pour chacun de ceux que vous connaissez, précisez dans quel(s) protocole(s) ils sont encapsulés.

7. Décrivez le processus d'ouverture d'une page web: but des différents paquets et protocoles aux différentes couches. (Rappelez vous vos TP de R1!)

8. Donnez le temps entre le « HTTP GET » et le premier « HTTP OK »

9. Donnez l'adresse IP de kheops.unice.fr et de votre machine. Comment s'assurer que les paquets que vous analysez sont bien les vôtres, et non ceux du binôme voisin qui fait le même TP ?

ICMP

Utilisez vos notes de cours sur ICMP, en particulier, les types de paquets ainsi que la signification du TTL (ou n'hésitez pas à aller chercher ces informations sur le web).

9. Enregistrez un ping vers kheops.unice.fr. Sélectionnez le premier « ICMP Echo Request », étendez les informations sur la partie de protocole IP : retrouvez votre adresse IP.

10. Combien d'octets contient l'en-tête IP ? Combien d'octets contient la charge de datagramme IP (encore appelée payload, pour « partie utile ») et comment déterminez-vous ce nombre ?

11. Le datagramme IP a-t-il été fragmenté ? Comment le déterminez-vous ?

12. Utilisez la commande `man traceroute` dans la console pour connaître le détail de traceroute. A quoi sert traceroute, et comment s'utilise t-il ? Que doit exactement renvoyer traceroute ? Lancez un traceroute vers kheops.unice.fr

13. Enregistrez maintenant un traceroute vers www.google.fr : que voyez-vous exactement ? Est-ce le résultat attendu, pouvez-vous dire que ce traceroute a réussi ? Nous allons dans ce qui suit identifier la raison de cela.

Pour contourner le problème, dans la suite, vous utiliserez l'enregistrement wireshark d'un traceroute fait à partir d'une machine située l'extérieur du réseau local. Ouvrez le fichier traceroute.cap dans wireshark. S'il ne se trouve pas déjà sur votre machine, récupérez-le sur ftp://lserver.tp405/traceroute.cap, avec le login etudiant/Etudiant007, ou par « *scp* etudiant@lserver.tp405*:traceroute.cap . »* dans la console,

14. Quelle est l'adresse IP de la machine qui a été utilisée ?

15. Quel est le nom et l'adresse IP du serveur ciblé par traceroute ?

16. Quel protocole est utilisé par la machine cliente dans le cadre de traceroute ? Quel est le

protocole utilisé pour la réponse à cette machine ?

17. Dans les résultats obtenus, quels champs des datagrammes IP changent TOUJOURS d'un message à l'autre ? Quels champs doivent rester constant, quels champs doivent changer ?

18. Trouvez la série de messages ICMP indiquant un TTL trop grand (TTL exceeded) envoyés par le routeur le plus proche. Quelles sont les valeurs du champ d'identification et du champ TTL ?

19. Faire la liste de tous les routeurs traversés.

20. Décrivez précisément le fonctionnement de traceroute.

21. Quel était donc le problème en question 13 ? (Pensez à la configuration du réseau local...)

Fragmentation

20. Utilisez la commande ping (voir `man ping`) avec une taille de paquet de 1472, puis 1473 puis 3000; faites ces 3 captures successivement, et après chacune, analysez les données ci-dessous pour répondre aux questions suivantes.

21. Observez les champs *IP id,* et les différents *flags* (à dérouler): à quoi correspondent-ils ? Quelle est la valeur du segment offset et pourquoi ?

22. Analysez le détails de IP et ICMP, pour comprendre la différence entre ce qu'il se passe pour 1472 et 1473. Notamment à quoi correspond 1518 ? (Pensez headers: allez chercher toutes les tailles d'entêtes pour pouvoir répondre).

Ethernet - ARP

Utilisez vos notes de cours sur ARP (ou informations appropriées sur le web). Faites un accès web sur www.mit.edu et capturez les paquets correspondants. On s'intéresse uniquement à la partie Ethernet.

22. Quelle est l'adresse Ethernet de votre machine ?

23. Quelle est l'adresse de destination indiquée dans la trame Ethernet ?

24. Est-ce l'adresse Ethernet du serveur www.mit.edu ? Pourquoi ? A quelle machine correspond cette adresse ?

25. Dans le message de réponse HTTP, quelle est la valeur de l'adresse Ethernet source ? À quelle machine correspond cette adresse ?

26. En utilisant la commande `arp -a`, affichez le contenu de la table arp.

27. Qu'est-ce qu'une table ARP ?

28. Videz la table arp (`arp -d @IP`).

29. Allez sur le site www.unice.fr, capturez les échanges et décrivez les échanges ARP en détail et leur but.

TP 5 - Wireshark : analyse de DHCP, FTP, SSH, mail

Connectez-vous sur votre compte (chaque étudiant du binôme sur un PC différent, sur son compte perso). Dans un terminal, exécutez
`createvm-gm VMTP5 Debian6admin-201303.SATA.vdi eth1 100 SATA`
Une fois la machine créée, regénérez son adresse MAC.
Logins et mdp habituels : rt/rt
Vous pouvez relire la partie introductive du TP 4 pour lancer wireshark. Tout se fait sur les machines virtuelles.

Étude de DHCP

L'objectif de cette partie est d'observer précisément le mécanisme de configuration réseau automatique, ou DHCP. Reprenez votre cours sur DHCP et ouvrez la page suivante :
http://en.wikipedia.org/wiki/Dynamic_Host_Configuration_Protocol
Sur un des 2 PC du binôme l'interface va être désactivée et ré-activée, et l'autre PC va observer le trafic, ce qui est rendu possible car vos 2 PC sont connectés à un hub au bout de la paillasse.

- Lancez une capture wireshark en mode promiscuous (cf. TP4) sur PC1, et sur PC2 arrêtez et de redémarrez les fonctions réseau (`ifconfig eth0 down` puis `ifconfig eth0 up`).

Examinez la capture pour décrire en détails le protocole DHCP :

1. Que signifie l'acronyme DHCP ?
2. Quel est le but exact du processus DHCP ?
3. Citez les 4 étapes du processus de configuration dynamique DHCP avec une description rapide de chacune d'elles.
4. Dans la capture identifiez et isolez chacun les paquets correspondant à chaque étape (attention de regarder les paquets correspondant bien à PC2, vous pouvez voir d'autres configurations d'autres PC de la salle qui démarrent, mais ne vous intéressent pas).
5. Pour chacun des ces paquets, rentrez dans le détail du protocole DHCP (Bootp), et observez que vous avec bien des formats de paquets et informations de la même forme que sur la page de wikipédia ci-dessus.
6. Pour chaque étape, donnez tous les **paramètres qui sont demandés** par le client au serveur, et donnez les valeurs que renvoie le serveur pour ces paramètres, spécifiques au réseau de la salle 405.

Étude de FTP

1. Donnez la signification de l'acronyme FTP.
2. Lancer une capture. Lancer une session ftp sur lserver.tp405 (`ftp lserver.tp405`), sous le login *etudiant* et password *Etudiant007*. Faites un `ls`. Puis `quit`. Arrêtez la capture.
3. Analyse de la capture : regarder les paquets FTP successifs et analyser leur contenu (donc au niveau application. Que dire du mot de passe ?
4. Que voyez vous dans la 2ème sous-fenêtre pour le détail de FTP ?
5. Quel est le rôle de TCP dans cet échange ?
6. Faites une analyse détaillée des ports TCP impliqués dans ces échanges, en rapport avec les commandes appelées.
7. Enfin, utiliser l'option *Follow TCP stream* sur les connexions d'intérêt.

Étude de SSH

1. Lancer une session ssh sur lserver.tp405: ssh etudiant@lserver.tp405.
2. Qu'observez-vous dans la trace ? Quel port TCP est à remarquer ?

Étude du protocole mail

1. Installez kmail depuis la logithèque (dans Système/Administration).
2. Utilisez Kmail comme client mail (`kmail &` dans une console) :
    1. Configurez un nouveau compte avec le nom d'utilisateur etudiant, adresse etudiant@lserver.tp405, serveur entrant (POP3) lserver.tp405 serveur sortant (SMTP) lserver.tp405.
       POP: encryption : TLS for secure dl, Authentication methode : Plain
       SMTP : encryption : TLS, no authentication
    2. Effectuez une capture (wireshark) d'envoi et de réception d'emails. Analyser le protocole utilisé. Peut-on retrouver le mot de passe en analysant les paquets reçus ? Observez attentivement le protocole SMTP.
    3. Quels sont les ports TCP spécifiques à SMTP et POP ?

3. On va à présent utiliser une connexion telnet au serveur email pour envoyer et recevoir :
    1. telnet lserver.tp405 25 → d'où vient ce numéro ?
    2. helo lserver.tp405
    3. mail from: etudiant@lserver.tp405
    4. rcpt to: etudiant@lserver.tp405
    5. data
    6. blabla
    7. .
    8. quit
    9. Et pour recevoir :
    10. telnet lserver.tp405 110 → d'où vient ce numéro ?
    11. user etudiant
    12. pass Etudiant007
    13. list
    14. retr [numero de message]
    15. quit
    16. Observez la capture: qu'est-ce qui change par rapport à l'utilisation d'un client comme Kmail, à l'émission et à la réception ?

Utilisation des outils du menu *Statistics* pour l'analyse de trafic

1. Effacez la table ARP, lancez une capture et lancez une session http (web). Après capture, donnez le détail de tous les protocoles utilisés au cours de l'échange via l'outil *flow graphs*.
2. Faites une capture sur 2 minutes, en générant le plus de trafic différencié possible (download d'ubuntu par exemple).

3. Utilisez l'outil *IO Graphs* avec différents filtrages et indiquez les trafics captés.

4. Sur la même capture, utilisez les outils *Conversation*, *Endpoints*, et *Protocol hierarchy*.

5. En fonction des résultats, faites un bilan complet avec, d'une part, l'analyse du trafic, et d'autre part, les indications sur les protocoles utilisés et leurs interactions.

TP 6 – Remote Network MONitoring : analyse de trafic avec RMON

Introduction à la surveillance et analyse de trafic:

A l'heure actuelle, les réseaux d'entreprise sont composés de plusieurs types de réseaux interconnectés. Les entreprise utilisent une grande variété de systèmes et d'applications sur ces réseaux. L'équipe d'administrateurs réseau doit être capable de fournir un environnement opérationnel, sécurisé, fiable (peu de pannes, peu d'impact si panne, et rapidement corrigée) et efficace pour supporter les activités quotidiennes de l'entreprise.

De plus, surveiller le trafic à un ou plusieurs endroits dans les réseau d'un opérateur (Orange, etc) permet à l'opérateur de comptabiliser le trafic, d'identifier des applications qui posent problème (comme le P2P), d'identifier la source des problèmes et les corriger, et de faire de l'ingénierie de trafic (comment répartir le trafic sur le réseau).

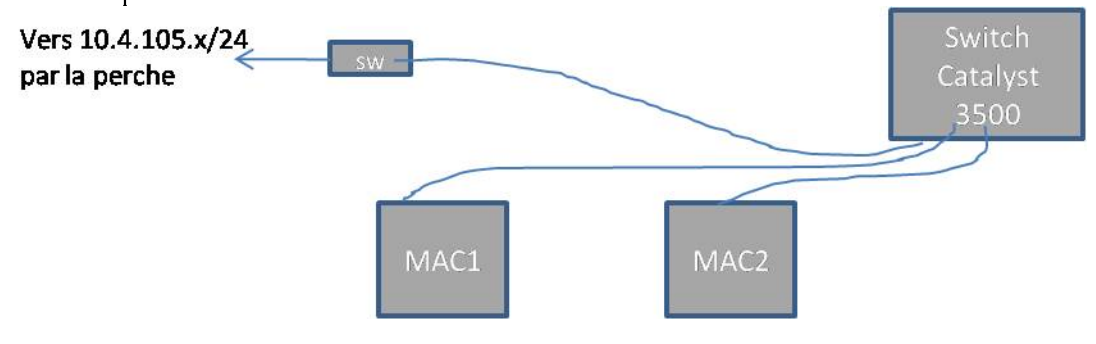
Surveillance avec RMON :

Dans les TP1, 4 et 5 notamment, le logiciel Wireshark est utilisé pour contrôler la carte réseau de la machine, et récupérer le trafic vu par cette carte, donc passant sur le câble relié au PC en question. Le logiciel permet ensuite une analyse du trafic.
Certains matériels, équipements spécialisés, ou switch et routeurs, peuvent eux-même analyser le trafic les traversant, et renvoyer des informations sur ce trafic vers une machine d'administrateur. L'intérêt est de pouvoir facilement surveiller le trafic à des endroits du réseau où la machine administrateur ne se trouve pas. Pour ce faire, ces équipements doivent implémenter des « modules » leur permettant de générer des informations sur le trafic qui les traverse. RMON est un des ces modules, Netflow, étudié dans le TP7, en est un autre.

RMON est un standard signifiant Remote MONitoring. Un équipement implémentant RMON est donc un agent qui va pouvoir être interrogé par une sorte de client, et ce grâce au protocole SNMP (Simple Network Management Protocol). Ce client récoltant les informations est appelé le manager SNMP. Vous verrez en fin de TP que RMON est une MIB, ou Management Information Base, normalisée, qui correspond à une structure en arbre aux différents niveaux duquel se trouvent des variables, dont la valeur peut nous intéresser et que l'on récupère donc.

Au lieu de travailler directement en lignes de commande avec le protocole SNMP pour récupérer les informations de l'agent, nous allons utiliser une interface graphique permettant ce dialogue avec l'agent RMON. Cette interface graphique est le logiciel Meterware, qui va tourner sur votre machine.

Dans tout ce qui suit, l'agent RMON sera pour ce TP un switch Cisco Catalyst 3500, et sera appelé « sonde ».
Schéma de votre paillasse :



Identifiez-bien quels ports du switch Catalyst 3500 correspondent à quelles machines.
Pour toutes les manipulations de ce TP, vous avez à votre disposition le manuel d'utilisation de METERWARE.

Chaque étudiant prend un MAC. Ouvrez la VM Windows PourTP6_R4.

Configuration de l'agent RMON : le switch Cisco Catalyst 3500

Vous allez d'abord devoir configurer le switch pour activer l'agent SNMP RMON.
Le switch dispose d'une adresse IP à laquelle vous pouvez le joindre via le réseau, en ouvrant une session telnet sur 10.4.105.171. Les mdp sont *cisco*. Vous pouvez faire ceci de la console Windows, ou depuis un terminal de la machine hôte.

Activation de SNMP et configuration des communautés :
En mode configuration:
```
snmp-server community public rw
snmp-server host @IP public
snmp-server enable traps
```
où `@IP` est l'adresse IP de la machine sur laquelle vous récupérez les informations de trafic.

Port monitoring :
Sur l'interface sur laquelle le trafic va être surveillé, vous allez également rediriger le trafic des autres interfaces :
```
interface FastEthernet0/1
port monitor FastEthernet0/2
port monitor FastEthernet0/3
port monitor VLAN1
```
Adaptez ces commandes pour l'autre MAC.
Lancez wireshark :
1. Quel effet ont les 3 commandes que vous venez de faire sur le switch : que vous attendez-vous à avoir sur la carte réseau de votre machine ?
2. Wireshark est-il capable de le voir dans la configuration de base ? Pourquoi ?
3. Comment configurer Wireshark pour voir le trafic de tous les ports sur votre machine ?
4. Le faire, vérifier et faire valider par l'enseignant.

Activer RMON sur l'interface FastEthernet0/1
C'est-à-dire celle sur laquelle est connectée votre machine.
```
rmon collection statistics 1
rmon collection history 1
```

En revenant en mode enable, la commande `show rmon stat` ou `show rmon history` (ou `show rmon alarms` plus tard) doit vous permettre de constater l'activation, par notamment la création des statistiques (comptage des paquets...).

Configuration et analyse rapide dans Meterware

Dans cette partie du TP, vous utiliserez la partie *Network map* pour dessiner un plan de la partie qui vous intéresse du réseau la salle TP405, en se basant sur la description du réseau de la salle en début du fascicule de TP. Y figurera :
- les 2 machines à votre disposition

- le switch Cisco Catalyst 3500 à IP fixe, qui est l'agent RMON, lié à ce hub
- le switch de la salle de brassage qui est relié à ce switch par la perche
- le serveur et la passerelle (pas reliés directement au switch)

1. Récupérez les adresses IP et MAC de vos 2 machines.

2. Pour ajouter des équipements dans *Network map*, faire *Edit* → *New device*

3. Ajouter d'abord la sonde, puis les autres équipements. La sonde étant un équipement supportant SNMP, vous pouvez ne rentrer que le nom et l'@IP, appuyer sur *resolve* et les informations sont récupérées. Changez les communautés de lecture et écriture à *public*.

   Une fois toute la topologie créée, cliquer sur la fonction Quick View de la sonde :

4. Comment la sonde estime t-elle l'état (la valeur) d'une variable que Meterware récupère ? Faites varier le *Sampling interval* (à trouver dans le menu) pour inférer la réponse.

5. A quoi correspond le premier graphique Packets/s : de quels types de paquets s'agit-il exactement (quelle couche OSI) ? Que représentent les ordonnées ? Que représente le nombre 1518 ?

6. Comment est calculée l'*utilisation* affichée en pourcentages (quelles sont les quantités concrètes qui interviennent dans ce calcul – débits impliqués) ?

Groupe « ALARM/EVENT »

Depuis Meterware :

1. Depuis le menu de la sonde, créer une alarme indiquant un dépassement de charge du réseau de 10%, c'est-à-dire un débit utilisé supérieur à 10 % du débit maximum (qui est 10 Mbps) :
   - Indiquez les paramètres que vous choisissez pour configurer cette alarme (*Variable, Sample interval, Rising et Falling thresholds*). En particulier :
   - Donnez le calcul exact vous permettant de déterminer le R*ising threshold*.

2. Générez un trafic important (par exemple download d'Ubuntu) et vérifiez que l'alarme a bien été déclenchée (dans les logs). Si l'alarme ne se déclenche pas, pensez à regarder votre débit de téléchargement par exemple, et à baisser le seuil de l'alarme le cas échéant pour voir le déclenchement.

Depuis le Switch :

5. Toujours au travers de la connexion telnet, utiliser les commandes `show rmon alarms`, `show rmon events`, et comparez à ce que vous voyez dans Meterware : Que voyez-vous et que constatez-vous ?
6. Effacez à présent l'alarme depuis Meterware, et reconfigurez la même mais directement en ligne de commande depuis le switch. Aidez-vous pour cela de la page suivante :

http://www.cisco.com/en/US/tech/tk961/technologies_configuration_example09186a0080094478.shtml
En particulier, à quoi correspond *alarmVariable* de cette page ?
Donner la totalité de la configuration de l'alarme. Appelez l'enseignant pour qu'il vérifie vos

réponses à cette question.

7. Regardez ensuite l'effet dans Meterware : que constatez-vous ?

8. A l'aide du point précédent et du manuel, créez les alarmes suivantes, directement à partir du menu de la sonde :
   1. charge supérieure à 20% de la bande passante
   2. charge inférieure à 30% de la bande passante
   3. nombre de paquets de taille supérieure à 1024 supérieur à 100 par seconde
   4. nombre de collisions compris entre 10 et 100 par seconde

   Pour chaque point, indiquez dans le rapport les valeurs exactes mises dans chaque case de configuration de l'alarme. Donner si possible le *alarmVariable* correspondant à chaque cas, en indiquant comment vous l'obtenez.

Groupe « statistics » de la sonde RMON (groupe RMON)

Consultez les pages afférentes au groupe Statistics dans le manuel de Meterware.

5. Dans un premier temps, réinitialisez les données de la sonde. Indiquez comment vous faites. Quelle est l'influence sur les mesures ?

6. Parcourez chaque fonction (dans l'onglet *View*) du menu Statistics.
7. Vous pouvez utiliser votre PC et/ou le PC de gauche pour générer du trafic de façon à, par exemple, voir des erreurs.

8. Détaillez ce que permet de représenter chaque fonction (et chaque sous graphique donc). On ne vous demande pas de recopier, mais de montrer que vous avez saisi la signification des graphiques. Indiquez notamment comment sont calculées les quantités représentées.

9. Notamment, quel est la différence entre mesure instantanée et mesure cumulative ?

TP 7 – Analyse de flux et outils Netflow : Nfdump et Nfsen

Introduction à la surveillance et analyse de trafic:

A l'heure actuelle, les réseaux d'entreprise sont composés de plusieurs types de réseaux interconnectés. Les entreprise utilisent une grande variété de systèmes et d'applications sur ces réseaux. L'équipe d'administrateurs réseau doit être capable de fournir un environnement opérationnel, sécurisé, fiable (peu de pannes, peu d'impact si panne, et rapidement corrigée) et efficace pour supporter les activités quotidiennes de l'entreprise.

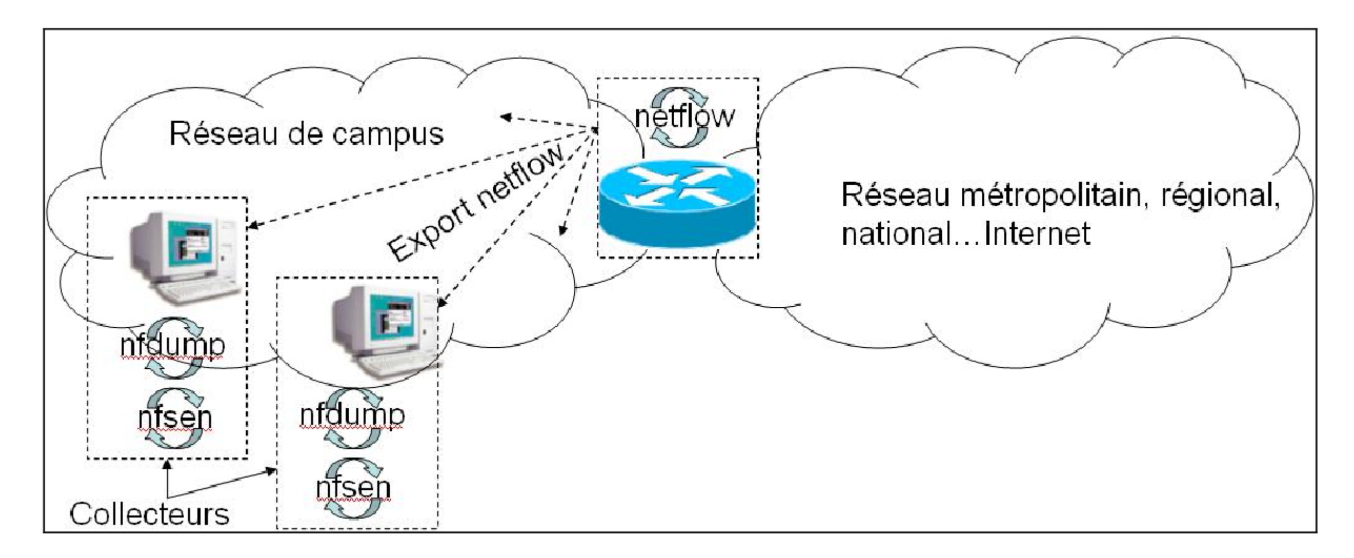
De plus, surveiller le trafic à un ou plusieurs endroits dans les réseau d'un opérateur (Orange, etc) permet à l'opérateur de comptabiliser le trafic, d'identifier des applications qui posent problème (comme le P2P), d'identifier la source des problèmes et les corriger, et de faire de l'ingénierie de trafic (comment répartir le trafic sur le réseau).

Contexte :

Netflow est un outil Cisco qui permet à un routeur d'exporter vers un collecteur des informations sur les flux IP le traversant.

Définition : un flux IP est un ensemble de paquets IP ayant en commun le quadruplet (Src IP, Src Port, Dst IP, Dst Port). Si le temps entre 2 paquets successifs ayant ces propriétés est supérieur à un certain seuil (par exemple 5 min), on considère que les nouveaux paquets font partie d'un deuxième flux. Le seuil est un paramètre à fixer.

Ces informations sur les flux le traversant sont envoyées, sous la forme de trames Netflow (version 5 ou 9) vers un (ou plusieurs) collecteurs selon le schéma suivant :



L'analyse des flux est réalisée avec le logiciel Nfdump qui fonctionne en ligne de commande. Il y a également une interface graphique à cet outil, qui s'appelle Nfsen (outil graphique se basant sur nfdump). Nfsen sera abordé en second.
(Plus d'infos à : http://nfdump.sourceforge.net/ et http://nfsen.sourceforge.net/ et man pour les options de chacun des outils)

L'outil Nfdump :

Nfdump est un ensemble d'outils en ligne de commande permettant la collecte, le stockage et le traitement des enregistrements de flux, compatibles avec netflow v5, v7, v9 et sflow. Les commandes importante de cette suite sont :

- **nfcapd** - Capture des netflow venant du routeur et enregistrement cyclique sous la forme de fichiers. Une rotation automatique sur les fichiers s'effectue (par défaut toutes les 5mn.).
- **nfdump** – Traitement des fichiers générés par nfcapd. Récupère les enregistrements de flux stockés par nfcapd pour effectuer des mesures/statistiques (top N par IP, ports…). (La syntaxe d'utilisation est similaire à celle de tcpdump ou wireshark.)

Les enregistrements de flux collectés sont stockés, par défaut toutes les 5 min, dans un nouveau fichier sous la forme : *nfcapd.YYYYMMddhhmm*. Par exemple, le fichier *nfcapd.200709181140* contient les données collectées le 18 sept. 2007 de 11h40 à 11h45.
Pour distinguer les enregistrements de flux provenant de routeurs différents, on les répartit dans des répertoires différents. Pour le TP, un routeur exportera des trames netflow, ensuite une de vos machine virtuelle exportera des données Netflow. Ce qui fera donc d'abord 1 puis 2 sources.

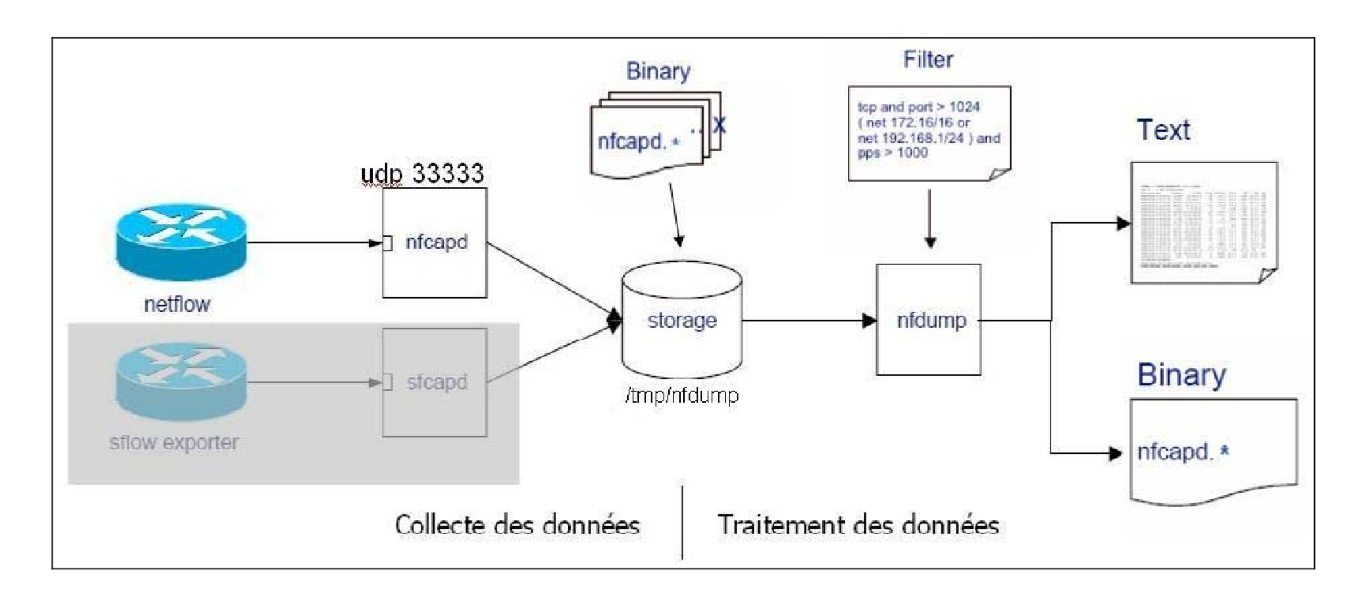
1. La **collecte** est effectuée par nfcpad en écoute sur le port (UDP 3333 ou 3334 pour le TP) à destination duquel le routeur (ou la machine exportant en netflow) exporte ses enregistrements de flux : `nfcapd -w -D -l /home/nfdump -p 3333`
   D : mode Daemon
   -*w* : permet de faire une rotation des fichiers de manière arrondie. Pour une valeur par défaut de l'intervalle de rotation qui est de 5mn, la rotation des fichiers s'alignera sur 0, 5,10...
   -*l* /tmp/nfdump : répertoire de stockage des données reçues sous forme de fichier nfcapd.*.
   -*p* en écoute sur le port 3333

2. L'**analyse des données** netflow avec Nfdump peut être faite sur un simple fichier (option –*r*) ou sur un ensemble de fichier (option –R) :
   ```
   nfdump -r /tmp/netflow/nfcapd.YYYYMMddhhmm
   nfdump -R /tmp/netflow/nfcapd.YYYYMMddhh00:nfcapd.YYYYMMddhh55
   ```

- **Aggrégation de flux** : pour simplifier le format d'affichage, on peut agréger les flux grâce à l'option *–a* qui réunie sur une même ligne les flux ayant les mêmes caractéristiques suivantes : protocole, adresse IP source et destination, port source et destination. Il est possible de n'agréger qu'en fonction de certaines caractéristiques avec l'option –A <scheme>, par exemple n'agréger les flux qu'en fonction de l'adresse IP src et du port destination s'exécute avec l'option `-a -A srcip,dstport`.

- **Filtrage** : En fonction des besoins (Analyse d'incident, détection de scans, pistage d'une machine, métrologie par port/srcip.../tos), Nfdump peut filtrer (sélectionner) les flux affichés. Par exemple, si on ne souhaite afficher que le trafic http à destination du serveur 10.0.2.3 sur une période d'1/2h :
  ```
  nfdump -R /tmp/netflow/nfcapd.Y…hh00:nfcapd.Y…hh30 'dst ip 10.0.2.3 and dst port 80'.
  ```

- **Statistiques Top N** : L'option `-s type[/orderby]` permet de faire des top N sur les enregistrements de flux (où N est configurable avec l'option `-n num`, `-n 0` affiche tous les enregistrements) en fonction d'une caractéristique (*type* : ip, proto, dstip, srcip, srcport…) et de manière ordonnée (*orderby* : décroissant par nombre de flux, nombre d'octets, de paquets…).



Partie 0 : Créer votre machine virtuelle

Connectez-vous sur votre compte (chaque étudiant du binôme sur un PC différent, sur son compte perso). Dans un terminal, excécutez
`createvm-gm VMTP7_1 Debian6admin-201303.SATA.vdi eth1 100 SATA`
Regénérez l'adresse MAC.
Logins et mdp habituels : rt/rt

Partie 1 : Installation de Nfdump

<u>Dépendances à installer au préalable</u> :
Utiliser *Synaptic Package Manager*, ou `apt-get install` pour installer les packages : rrdtool, apache2 (il va falloir qu'un serveur http tourne sur votre machine), libapache2-mod-php5, flex, librrd-dev, byacc-j, librrdtool-oo-perl, libio-socket-inet6-perl.

<u>Installation de Nfdump</u> :

Télécharger Nfdump depuis : http://sourceforge.net/projects/nfdump/
le décompreser et l'installer :

```
tar -zxvf nfdump-1.6.6.tar.gz
cd <repertoire_créé>
```

Passer en mode root

```
./configure --enable-nfprofile --enable-nftrack
make
make install
```

S'il y a une erreur, c'est très probablement dû à une dépendance qui n'a pas été installée correctement. Lisez le message d'erreur et remédiez au problème.
Après l'installation, assurez-vous que les fichiers suivants soient installés. Dans */usr/local/bin*, vous devez au moins trouver : *nfdump, nfcapd, nfexpire, nfprofile, nftrack*.

Partie 2 : Configuration du routeur

Vous devez configurer le routeur Cisco 2621XM au dessus de vous pour qu'il exporte des

informations sur les flux IP le traversant, sous la forme de données Netflow, avant d'analyser ces données grâce à Nfdump.

Vous accédez au routeur par telnet. Son @IP est 10.4.105.170. Mot de passe : cisco

En mode enable et configuration, faire :

1. To enable netflow in router

- interface fastethernet 0/0
- ip route-cache flow

En retournant dans le mode configuration générale :

2. Send netflow data

- ip flow-export destination <ip-address> <udp-port>
- ip flow-export version 5
- ip flow-cache timeout active 5

Timeout est la durée maximale d'un flow IP, avant que le routeur ne casse ce flow s'il est plus long. Ne pas modifier ce paramètre.

Garder la connexion telnet ouverte, lancer un ping vers le routeur et connectez-vous sur http://10.4.105.170 (depuis la VM ou la machine hôte). Garder ces 3 connexions ouvertes et actives pour toute la suite du TP.

Partie 3 : Capture de données Netflow du routeur et filtrage par Nfdump

3. Faire fonctionner nfcapd et nfdump

Wireshark

Avant de lancer ces commandes nfdump, assurez-vous que le routeur est bien en train d'envoyer des packets vers votre machine, sur le bon port UDP. Utilisez Wireshark pour cela, et ajouter un filtre sur l'adresse du routeur : ip.addr = = 10.4.105.170. Les flux collectés depuis le routeur sont des paquets UDP.

Nfcapd

Nfcapd peut être lancé par tout utilisateur dans le répertoire de stockage voulu : prenez */home/rt/nfcaptures* (à créer).

- `nfcapd -w -t 300 -p 3333 -l /home/rt/nfcaptures &`

-w => crée un nouveau fichier à chaque intervalle de -t *5* minutes (300s), en écoutant les paquets à destination du port *-p 3333* , dans le répertoire *-l output directory.*

Plus d'options avec

- `nfcapd -help`

Vérifiez qu'un processus nfcapd a bien été lancé en écoute sur le port UDP 3333 :

- `netstat -lu -p`

4. NfDump

Pour voir les données capturées par nfcapd :

- `nfdump -r /home/rt/nfcaptures/nfcapd.(timeslot)`

où `nfcapd.(timeslot)` est un fichier particulier, ou

- `nfdump -R /home/rt/nfcaptures/nfcapd.(timeslotdébut):/home/rt/nfcaptures/nfcapd.(timeslotfin)`

En vous servant des 2 premières pages de l'énoncé du TP, de http://nfdump.sourceforge.net/, et de la commande `nfdump --help` , répondez aux questions suivantes en indiquant dans le rapport les commandes que vous avez utilisé, et la réponse éventuelle à la question « Trouver ».

- Pour un fichier d'enregistrement de flux de 5mn :
  - Afficher les flux

Q1: `nfdump -r nfcapd._ _ _ _ _ _ _ _ _ _`

  - Afficher les statistiques par protocole (regroupement des flows par protocole de couche 4).

Q2: `nfdump -r nfcapd._ - _ _ _ _ _ _ _`

  - Afficher les flux de manière agrégée et repérer le couple srcip, dstip comportant le plus de flux

Q3: `nfdump -r nfcapd._ - _ _ _ _ _ _ _ _`

Q4: A quoi ces flux correspondent-ils ?

- Sur une période de 10mn : filtres et recherche
  - Afficher seulement les flux à destination du port TCP 80

Q5: `nfdump -R nfcapd._ _:nfcapd._ _ _ - _ '_ _ _ _'`

  - Quelle est l'adresse IP du serveur utilisant le port TCP 23 ?

Q6: `nfdump -R nfcapd._ _:nfcapd._ _ _ _ _ _`

  - A quoi correspondent les flux avec le port UDP 67 ?

Q7: `nfdump -R nfcapd._ _:nfcapd._ _ _ _ _ _ _ _ _ _ _ _ _ _ _`

Stopper nfcapd : en mode root, `nstat -lu -program` et `kill -9 <PID>`.

Partie 4 : Installation de Nfsen

Pour éviter de devoir extraire en ligne de commande les informations qui nous intéressent des Netflow, l'outil Nfsen permet d'avoir une interface Web pour interpréter graphiquement les fichiers générés par le processus nfcapd. Il s'agit donc d'installer la suite logicielle Nfsen, ainsi qu'un serveur Web local (Apache) pour au final visualiser les informations de trafic dans une page Web.

Télécharger Nfsen depuis http://sourceforge.net/projects/nfsen/ et le décompresser.

5. Créer un utilisateur nfsen et donner à l'utilisateur apache les permissions nfsen

Un nouvel utilisateur et un nouveau groupe sont créés pour permettre à des commandes externes de fonctionner depuis l'interface web.Vous devez être root pour effectuer les commandes suivantes.

- `/usr/sbin/useradd -m nfsen`

- `passwd nfsen` (prenez le login pour mdp)
- `/usr/sbin/groupadd nfsen`
- `/usr/sbin/usermod -G nfsen nfsen`

Create a new group and adding it to apache user group.

- `/usr/sbin/groupadd nfsenadmin`
- `/usr/sbin/usermod -a -G nfsenadmin nfsen` (adding user nfsen to nfsenadmin group)
- `/usr/sbin/usermod -a -G nfsenadmin www-data` (adding user apache to nfsenadmin group)

6. Créer un répertoire HTML DIR

Avant d'installer Nfsen, il faut encore créer un répertoire HTML où seront stockées les pages Web représentant les données Netflow.

- `mkdir –p /usr/local/nfsen/www/htdocs/nfsen`

Changer les droits du répertoire à *nfsen:nfsenadmin* pour ne pas avoir de problèmes de droit plus tard.

- `chown –R nfsen:nfsenadmin /usr/local/nfsen`

7. Configuration de Nfsen : le fichier *nfsen.conf*

Quand vous installez nfsen, ou changez sa configuration, tout se passe dans le fichier nfsen.conf situé dans le répertoire etc/. S'uy positionner :

- `cd /home/rt/Téléchargements/nfsen-1.3.6p1/etc`

Editez *nfsen-dist.conf* (avec gedit par exemple) et sauvegardez-le en *nfsen.conf* après avoir fait les changements suivants (ne pas toucher aux autres options) :

- $BASEDIR=”/usr/local/nfsen”
- $HTMLDIR=”${BASEDIR}/www/htdocs/nfsen”
- $USER=”nfsen”
- $WWWUSER=”nfsen”
- $WWWGROUP=”nfsenadmin”
- %sources = (

‘Router1’ => { ‘port’ => ‘3333’, ‘col’ => ‘#0000ff’, ‘type’ =>’netflow’ },) ;

Ne pas oublier d'enlever les autres sources (peer1 et peer2).

Puis :

- `cd ..`
- `./install.pl etc/nfsen.conf`

Et Nfsen est installé sur votre système.

8. Configurer l'interface web

Vous devez vous souvenir qu'Apache est un serveur HTTP open-source, qui va être utilisé par Nfsen. Créer un fichier *nfsen.conf* dans le répertoire */etc/apache2/conf.d*. Mettez-y les lignes suivantes :

alias /nfsen “/usr/local/nfsen/www/htdocs/nfsen”

<directory “/usr/local/nfsen/www/htdocs/nfsen”>
</directory>
Après avoir sauvé et fermé, redémarrez le serveur web : `/etc/init.d/apache2 restart`

9. Faire fonctionner Nfsen

Après l'installation, démarrer Nfsen : `/usr/local/nfsen/bin/nfsen start`

Pour le stopper : `/usr/local/nfsen/bin/nfsen stop`

Et connectez-vous sur *http://localhost/nfsen/nfsen.php*
Cliquez sur le premier graphique.
Les erreurs se voient dans le fichier syslog : tail /var/log/syslog

Partie 4 : Analyse dans Nfsen

Vérifiez que vous pouvez visualiser votre trafic, et refaire un des filtres de la partie précédente. Explorez les menus.

Créer un alerte :
En fonction des données netflow reçues du routeur, Nfdump est capable de déclencher des alarmes, configurées au préalable par l'administrateur réseau, et de prévenir celui-ci en cas de déclenchement. Les alarmes peuvent être configurées directement au travers de Nfsen. Documentez-vous sur le page de nfsen pour
Q8 : Créer une alarme se déclenchant si le nombre de flows par seconde dépasse la moyenne vue sur 10min, ou une valeur absolue que vous fixerez (vérifier qu'elle se déclenche bien dans ces conditions).

Partie 5 : Analyse de traces complexes

Rejouer les données Netflow envoyées par un routeur :

La surveillance du trafic est particulièrement importante sur les routeurs de bord, permettant l'accès à l'Internet. Nous allons analyser une telle trace.
Il va falloir télécharger (pas tout de suite) le premier fichier de la trace n°7 de http://www.simpleweb.org/wiki/Traces
Ce fichier n'est pas une capture réalisée par nfcapd, c'est-à-dire un fichier nfcapd, mais un fichier pcap, correspondant à une capture, réalisée avec tcpdump ou wireshark, des trames envoyées par l'agent netflow du routeur.
Pour analyser le trafic de ce routeur de bord d'université, il va donc falloir d'abord re-créer les fichiers lisibles par nfdump, donc issus d'une capture par nfcapd.
Pour ce faire, vous allez modifier cette trace grâce à l'outil tcprewrite, et ensuite la rejouer grâce à tcpreplay, pour que nfcapd génère des fichiers de trace qu'enfin vous allez pouvoir analyser.

Créer une deuxième machine virtuelle, grâce à la même ligne de commande 'au début, sauf que vous changez le nom `VMTP7_1` pour `VMTP7_2`. Ré-initialisez son adresse MAC. Ce sera de cette VM *VMTP7_2* que vous allez rejouer le trafic vers la VM *VMTP7_1*. Pour cela :
- Sur VM1 :Modifier votre nsfen.conf de façon à permettre l'introduction d'une nouvelle source Netflow envoyant sur le port 3334.
- Sur VM2 (pour la suite) : Télécharger le premier fichier de la trace n°7 de http://www.simpleweb.org/wiki/Traces
- Installer tcpreplay (avec un apt-get install).

- Changement de l'adresse MAC de destination (la destination étant VM1) du trafic de la trace, pour que le trafic rejoué arrive bien sur VM1:
- `# tcprewrite --enet-dmac=@MACdest –infile=netflow`
- Génération d'un fichier intermédiaire pour changement d'adresses IP :
- `# tcpprep --auto=bridge --pcap=netflow –cachefile=input.cache`
- Changement de l'adresse IP de destination (la destination étant VM1) :
- `# tcprewrite --endpoints=@IPdest:@IPsource --portmap=9500:3334 –cachefile=input.cache –infile=outpu1.pcap --outfile=output.pcap`
- Rejouer cette trace Netflow avec la commande *tcpreplay* (en mode root).
- `# tcpreplay -i eth0 output.pcap`
- Afin de vérifier que VM1 reçoit bien les paquets Netflow (et ainsi crée bien ses fichiers nfcapd), lancer un Wireshark (ou tcpdump) sur VM1.

Analyser les données Netflow envoyées par le routeur

Utilisez une page Web répertoriant les ports TCP et UDP pour repérer les services dans les question suivantes. De même, aidez-vous de la page de Nfsen, notamment pour la syntaxe des filtres si vous avez des problèmes.

Q9- Avant même que la toute la trace soit rejouée, et au maximum pour les 20 premières minutes de trafic (qui arrive très vite sur votre VM_Netflow1), analysez les fichiers générés par nfcapd, en utilisant Nfsen (dans l'explorateur web que vous aviez lancé sur VM_Netflow1). Positionnez donc les curseurs de la fenêtre du trafic en conséquence.

Q10- En utilisant un filtre, faire afficher (« lister ») les flux à destination du port TCP 80 à l'aide d'un filtre.

Q11- Mesurer et écrire la quantité de bytes de ces flux en utilisant en plus une agrégation sur le protocole.

Q12- Trouver et écrire l'adresse IP des serveurs DNS, Web et NTP générant la majorité des flows grâce aux options de Stat TopN.

Q13- Afficher le Top 20 des connexions (c'est-à-dire les quadruplets (srcip,dstip,srcport,dstport)) par nombre d'octets des flux udp (voir éventuellement page web de Nfdump pour aide sur Top N stats). Ecrire les 2 premières.

Q14- Afficher le Top 20 des services par nombre de flux. Ecrire les 3 premiers.

Q15- A quoi correspondent les 3 premiers ?

Q16- Faire la même chose par nombre d'octets (i.e., quantité de trafic). Que constate-t'on quant au nombre d'octet pour ces 4 services, en comparaison du nombre de flux, et expliquez ?

Q17- Afficher le Top 10 des adresses IP les plus consommatrices en débit. Ecrire la première.

Q18- Donner la nature du trafic émis par la station la plus consommatrice (revenez dans List Flows pour cela).

Q19- Afficher et écrivez le Top 3 des réseaux /24 échangeant le plus de trafic .

<u>Utilisation du plugin php Port Tracker</u>

Pour l'installer, suivez les instructions de *Download/nfsen-1.3.6p1/contrib/PortTracker/INSTALL*.
Visualisez l'utilisation des ports de façon à répondre aux questions suivantes.
Attention : Pour pouvoir afficher les ports souhaités, vous devez désactiver (« *skip* ») les ports 65527 à 65535.

Q20- Quelle est la fraction de http et https par rapport au trafic tcp total ?

Q21- Sur quels 2 ports le trafic udp peut être majoritaire ? Vérifiez votre réponse.

Q22- Parmi smtp, pop, pops, imap, imaps, quel est l'ordre d'utilisation de ces protocoles mail ?